Introducción a la Criptografía Moderna

Criptosistemas basados en Curvas Elípticas (ECC)

Rodrigo Abarzúa[†],

[†]Universidad de Santiago de Chile
rodrigo.abarzua@usach.cl

April 22, 2014

Introduction

- In the last decade, the demand for wireless technology (cellular, PDA, smart card) increased significantly.
- If two parties, Alice (A) and Bob (B), want to send messages between themselves without and eavesdropper Eve (E) reading the messages.
- Private-key (symmetric) cryptography relies on establishing a know secret between A and B before they can communicate.
    - **¿What if, as often happen in practice, it is infeasible for A ad B to have a prearranged secret?**

Introduction

- In the last decade, the demand for wireless technology (cellular, PDA, smart card) increased significantly.
- If two parties, Alice (A) and Bob (B), want to send messages between themselves without and eavesdropper Eve (E) reading the messages.
- Private-key (symmetric) cryptography relies on establishing a know secret between A and B before they can communicate.
  - **¿What if, as often happen in practice, it is infeasible for A ad B to have a prearranged secret?**

Introduction

- In the last decade, the demand for wireless technology (cellular, PDA, smart card) increased significantly.
- If two parties, Alice (A) and Bob (B), want to send messages between themselves without and eavesdropper Eve (E) reading the messages.
- Private-key (symmetric) cryptography relies on establishing a know secret between A and B before they can communicate.
  - **¿What if, as often happen in practice, it is infeasible for A ad B to have a prearranged secret?**

Introduction

- In the last decade, the demand for wireless technology (cellular, PDA, smart card) increased significantly.
- If two parties, Alice (A) and Bob (B), want to send messages between themselves without and eavesdropper Eve (E) reading the messages.
- Private-key (symmetric) cryptography relies on establishing a know secret between A and B before they can communicate.
    - **¿What if, as often happen in practice, it is infeasible for A ad B to have a prearranged secret?**

Diffie-Hellman Key Exchange (Public-key)

- Public Directory

elements: G, g

- If **A** and **B** come up with private keys:

A

$\mathbf{a} \in \mathbb{Z}^+$ publishes: $k_A = [a] \cdot g$

B

$\mathbf{b} \in \mathbb{Z}^+$ publishes: $k_B = [b] \cdot g$

- Public Directory

elements: G, g, k_A, k_B.

- **A** and **B** computes:

A

$[a] \cdot k_B = [a]([b] \cdot g)$

B

$b \cdot k_A = [b]([a] \cdot g)$

- The Secret Between **A** and **B** is:

$$K_{AB} = [a]([b] \cdot g) = [b]([a] \cdot g) = K_{BA}$$

Elliptic Curve Cryptosystems (ECC)

An elliptic curve E over a field K is defined by the general Weierstrass equation:

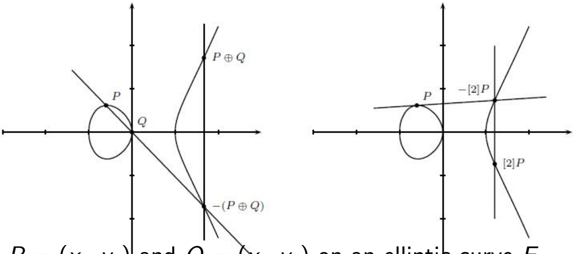
$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

where the coefficients $a_1, a_2, a_3, a_4, a_6 \in K$ and $\triangle \neq 0$, where $\triangle$ is the *discriminant of E*, $\triangle = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$ with

$$\begin{aligned} d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

If L is any extension field of K, then the set of $L-$*rational point* on E is the union of all point $(x, y) \in L \times L$ satisfying equation (1), together with a special point P_∞, called the point at infinity form an abelian group.

Group law on elliptic curve



Given two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on an elliptic curve E.

$$-P = (x_1, -y_1 - a_1 x_1 - a_3),$$

$$P \oplus Q = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3), \text{ where}$$

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } P \neq \pm Q, \\ \\ \dfrac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3} & \text{if } P = Q. \end{cases}$$

Theorem

The points on an elliptic curve together with P_∞ have cyclic subgroups. Under certain conditions all points on an elliptic curve form a cyclic group.

Gruop Order

Let E be an elliptic curve defined over $\mathbb{F}_p$. The number of point in $E(\mathbb{F}_q)$, denoted $\#E(\mathbb{F}_p)$, is called the **order** of E over $\mathbb{F}_p$.

Theorem (Hasse's)

Let E be an elliptic curve defined over $\mathbb{F}_p$. Then

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$

Hasses theorem, which is also known as Hasses bound, states that the number of points is roughly in the range of the prime p.

This has major practical implications:

For instance, if we need an elliptic curve with 2^{160} elements, we have to use a prime of length of about 160 bit.

Definition (Elliptic Curve Discrete Logarithm Problem (ECDLP))

Given is an elliptic curve E. We consider a primitive element P and another element T. The DL problem is finding the interger d, where $1 \leq d \leq \#E$, such that:

$$\underbrace{P + P + \cdots + P + P}_{d \ \ times} = [d] \cdot P$$

Is the fundamental operation of cryptosystems based on the DLP

Elliptic Curves over Prime Field $\mathbb{F}_p$, $char(\mathbb{F}_p) \neq \{2, 3\}$

When working with fields of characteristic is not 2 and characteristic is not 3, them we can transform the Weierstrass equation [**?**]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

If the characteristic of the fields is not 2, then we can divide by 2 and complete te square:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

which can be written as

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6',$$

with $y_1 = y + a_1x/2 + a_3/2$ and with some constants a_2', a_4', a_6'. If the characteristic is also not 3, then we can let $x_1 = x + a_2'/3$ and obtain

$$E : y_1^2 = x_1^3 + Ax_1 + B \tag{2}$$

for some constants A, B, where $A, B \in \mathbb{F}_p$ and $\triangle = 4A^3 + 27B^2 \neq 0$. The points $(x_1, y_1) \in \mathbb{F} \times \mathbb{F}$ satisfying the curve equations (points on the curve) in conjunction with the *point at infinity* P_∞ and the "cord-and-tangent addition" form a group that can be used to create elliptic curve cryptosystems (ECC).

Elliptic Curves over Prime Field $\mathbb{F}_p$, $char(\mathbb{F}_p) \neq \{2, 3\}$

Them we can transform the Weierstrass equation

$$E(\mathbb{F}_p) : y^2 = x^3 + ax + b \tag{3}$$

for some constants $a, b \in \mathbb{F}_p$ and $\triangle = -16(4a^3 + 27b^2)$.
Let $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E(\mathbb{F}_p)$ such that $P \neq \pm Q$

Addition: $P + Q = (x_3, y_3)$.

$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1, \qquad \lambda = \frac{y_1 - y_2}{x_1 - x_2}$

Doubling: $[2]P = (x_3, y_3)$

$x_3 = \lambda^2 - 2x_1, \qquad y_3 = \lambda(x_1 - x_3) - y_1, \qquad \lambda = \frac{3x_1^2 + a}{2y_1}$

The elliptic curve $E: y^2 = x^3 + 4x + 20$ defined over $\mathbb{F}_{29}$ has $\#E(\mathbb{F}_{29}) = 37$. Since 37 is prime, $E(\mathbb{F}_29)$ is a cyclic group and any point in $E(\mathbb{F}_{29})$ except for P_∞ is a generator of $E(\mathbb{F}_{29})$.

The following shows that the multiples of the point $P = (1,5)$ generate all the points in $E(\mathbb{F}_{29})$

$[0]P = P_\infty$	$8P = (8,10)$	$16P = (0,22)$	$24P = (16,2)$	$32P = (6,17)$
$[1]P = (1,5)$	$9P = (14,23)$	$17P = (27,2)$	$25P = (19,16)$	$33P = (15,2)$
$[2]P = (4,19)$	$10P = (13,23)$	$18P = (2,23)$	$26P = (10,4)$	$34P = (20,26)$
$[3]P = (20,3)$	$11P = (10,25)$	$19P = (2,6)$	$27P = (13,6)$	$35P = (4,10)$
$[4]P = (15,27)$	$12P = (19,13)$	$20P = (27,27)$	$28P = (14,6)$	$36P = (1,24)$
$[5]P = (6,12)$	$13P = (16,27)$	$21P = (0,7)$	$29P = (8,19)$	
$[6]P = (17,19)$	$14P = (5,22)$	$22P = (3,28)$	$30P = (24,7)$	
$[7]P = (24,22)$	$15P = (3,1)$	$23P = (5,7)$	$31P = (17,10)$	

Elliptic Curves over Binary Field $\mathbb{F}_{2^q}$, $(a_1 \neq 0)$

Them we can transform the Weierstrass equation

$$E(\mathbb{F}_{2^q}) : y^2 + xy = x^3 + ax^2 + b \tag{4}$$

where $a, b \in \mathbb{F}_{2^q}$ and $\triangle = b \neq 0$. Such a curve is said to be non-supersingular.
Let $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E(\mathbb{F}_{2^q})$ such that $P \neq \pm Q$

Addition: $P + Q = (x_3, y_3)$.

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \qquad y_3 = \lambda(x_1 + x_3) + x_3 + y_1, \qquad \lambda = \frac{y_1+y_2}{x_1+x_2}$$

Doubling: $[2]P = (x_3, y_3)$

$$x_3 = \lambda^2 + \lambda + a = x_1^2 + \frac{b}{x_1^2}, \qquad y_3 = x_1^2 + \lambda x_3 + x_3, \qquad \lambda = x_1 + \frac{y_1}{x_1}$$

Scalar Multiplication and DLP in ECC

- Given a finite additive cyclic group

G of order **n** generated by an element **P**.

- Given a positive integer

a and a element **P**, compute **[a]·P**

$$\underbrace{P + P + \cdots + P + P}_{a \text{ times}} = [a] \cdot P$$

Is the fundamental operation of cryptosystems based on the DLP.

This operation can be easily computed using the binary method at a cost of

$nD + \frac{n}{2}A$, where $|a| = n$

Scalar multiplications binary algorithm ($[d]P$)

Left-to-right Binary Algorithm

Algorithm 1: Left-to-right

`Input:` Point $\mathbf{P} \in E(\mathbb{F}_q)$, $k \in (k_{n-1}, \ldots, k_1, k_0)_2 \in \mathbb{N}$
`Output:` $\mathbf{Q} = [k] \cdot \mathbf{P}$

1. $R_0 \leftarrow \mathcal{O}$; $R_1 \leftarrow P$
2. **For** i **from** $n-1$ **to** 0 **do**
3. $R_0 \leftarrow 2R_0$
4. **If** $k_i = 1$ **then**
5. $R_0 \leftarrow R_0 + R_1$
6. **End If**
7. **End For**
8. **return** R_0

Right-to-Left Binary Algorithm

Algorithm 2: Right-to-Left

`Input:` Point $\mathbf{P} \in E(\mathbb{F}_q)$, $k \in (k_{n-1}, \ldots, k_1, k_0)_2 \in \mathbb{N}$
`Output:` $\mathbf{Q} = [k] \cdot \mathbf{P}$

1. $R_0 \leftarrow \mathcal{O}$; $R_1 \leftarrow P$
2. **For** i **from** 0 **to** $t-1$ **do**
3. **If** $k_i = 1$ **then**
4. $R_0 \leftarrow R_0 + R_1$
5. **End If**
. $R_1 \leftarrow 2R_1$
6. **End For**
7. **return** R_0

Example

Example:Consider $d = 78 = (1001110)_2$

Value of Step k	0	1	2	3	4	5	6
Value of d_{n-k}	1	0	0	1	1	1	0
Value of $S_k(P)$	P	$2P$	$4P$	$9P$	$19P$	$39P$	$78P$

Example

$[a]P = [104143711012733238876513676535587592720823664060901595554869421344539731012577]P$

$[(1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 0, 0,$
$1, 1, 1, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1,$
$1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0,$
$0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 0, 1, 1,$
$0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1,$
$1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 0, 0, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0,$
$1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 0, 1, 1, 0, 1,$
$0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 1)]_2 P$

Takes 255 doubling (D) and 123 Additions (A).

Why Elliptic curves??

- Increase performance by reducing the key size while keeping the same security. A security level s is achieved when we estimate that solving the instance will require more that 2^s operations.

Security level	80	112	128	192	256
ECC	160	224	256	384	512
RSA	1024	2048	3072	8192	15360

- Additional structure, example, Pairings-based cryptographic protocols.

$A = -3$, $E : y^2 = x^3 - 3x + B$

In our setting, the extra assumption is $A = -3$, which reduces the cost of the group doubling (as well as tripling and quintupling).
We will therefore assume that the elliptic curve E is defined over a (large) prime field given by the equation:

$$E : y^2 = x^3 - 3x + B \tag{5}$$

Projective Coordinates and the Group Law for Elliptic Curves

- The natural representation for a point on an elliptic curve group is the affine representation, i.e., by an ordered pair (x, y) of field elements satisfying the equation of the curve (the affine representation).

$$E : y^2 + a_1xy + a_3y = x_3 + a_2x_2 + a_4x + a_6$$

- Group operations in the affine representation require at least one field inversion, Let $P = (x_1, y_1)$ and $Q = (x_2, y_2) \in E(\mathbb{F}_p)$ such that $P \neq \pm Q$

Addition: $P + Q = (x_3, y_3)$.

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1, \qquad \lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

which is the most expensive of the elementary field operations 1I=100M.

- To avoid inversions, we can use projective coordinates (X, Y, Z) to solve that problem by incorporating a third coordinate Z and replace inversions with a few other field operations.

Projective Coordinates

- The natural representation for a point on an elliptic curve group is the affine representation.
- To avoid inversions, we can use projective coordinates (X, Y, Z) to solve that problem by incorporating a third coordinate Z and replace inversions with a few other field operations.

Let K be a field, and let c and d be positive integers. One can define an equivalence relation $\sim_{c,d}$ on the set $K^3 \setminus \{0,0,0\}$ of nonzero triples over K by

$$(X_1, Y_1, Z_1) \sim_{c,d} (X_2, Y_2, Z_2) \Leftrightarrow \text{there is}\, \lambda \,\text{in}\, K^* \,|\, X_2 = \lambda^c X_1,\ Y_2 = \lambda^d Y_1 \,\text{and}\, Z_2 = \lambda Z_1.$$

The equivalence class containing $(X, Y, Z) \in K^3 \setminus \{0,0,0\}$ is

$$(X : Y : Z) = \{(\lambda^c X, \lambda^d Y, \lambda Z) : \lambda \in K^*\}$$

The point $(X : Y : Z)$ is called a *projective point*, and (X, Y, Z) is called a *representative* of $(X : Y : Z)$. The set of all projective point is denote by $\mathbb{P}(K)$.

Example: Standard projective coordinates

Ejemplo

(standard projective coordinates) Let $c = 1$ *and* $d = 1$. *Then the projective form of the Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x_3 + a_2x_2 + a_4x + a_6$$

defined over K *is*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X_2Z + a_4XZ^2 + a_6Z^3.$$

To see what points on E *lie at infinity, set* $Z = 0$ *and obtain* $0 = X^3$. *Therefore* $X = 0$, *and* Y *can be any nonzero element (recall that* $(0 : 0 : 0)$ *is not allowed). Rescale by* Y *to find that* $(0 : Y : 0) = (0 : 1 : 0)$. *Then only point on the line at infinity that also lies on* E *is* $(0 : 1 : 0)$. *This projective point corresponds to the point* P_∞ *in definition (1).*

Projective coordinates $\mathcal{P}$

In projective coordinates, the equation of E is

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

The point $(X_1 : Y_1 : Z_1)$ on E corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$ when $Z_1 \neq 0$ and to the point at infinity $P_\infty = (0 : 1 : 0)$ otherwise. The opposite of $(X_1 : Y_1 : Z_1)$ is $(X_1 : -Y_1 : Z_1)$

Point Doubling in Projective Coordinates

Let $P = (X_1, Y_1, Z_1)$ be a point in Projective coordinates on can be computed $2P = (X_3, Y_3, Z_3)$ by the following formula with complexity :

$$A = aZ_1^2 + 3X_1^2, \qquad B = Y_1 Z_1,$$
$$C = X_1 Y_1 B, \qquad D = A^2 - 8C,$$

and

$$X_3 = 2BD, \qquad Y_3 = A(4C - D) - 8Y_1^2 B^2,$$
$$Z_3 = 8B^3.$$

Point Addition in Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ be points in Jacobian coordinates on the elliptic curve E. The point addition $P + Q = (X_3, Y_3, Z_3)$, can be computed by:

$$A = Y_2 Z_1 - Y_1 Z_2, \quad B = X_2 Z_1 - X_1 Z_2, \quad C = A^2 Z_1 Z_2 - B^3 - 2B^2 X_1 Z_2$$

so that

$$X_3 = BC, \quad Y_3 = A(B^2 X_1 Z_2 - C) - B^3 Y_1 Z_2, \quad Z_3 = B^3 Z_1 Z_2.$$

the cost of the general addition is

Example: Jacobian coordinates

Ejemplo

(Jacobian coordinates) Let $c = 2$ *and* $d = 3$*. Since to each (affine) point* $P = (x, y)$ *we can associate all triples* $(xZ^2 : yZ^3 : Z)$ *with* $Z \neq 0$*, and all those triples are valid.*
The projective point $(X : Y : Z)$*,* $Z = 0$*, corresponds to the affine point* $(X/Z^2, Y/Z^3)$*.*
The projective form of the Weierstrass equation

$$E : y^2 = x^3 + ax + b$$

defined over K *is*

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

The point at infinity P_∞ *corresponds to* $(1 : 1 : 0)$*, while the negative of* $(X : Y : Z)$ *is* $(X : -Y : Z)$*.*

Point Doubling in Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1)$ be a point in Jacobian coordinates on can be computed $2P = (X_3, Y_3, Z_3)$ by the following formula with complexity $4M + 4S$:

$$\alpha = 3(X_1 + Z_1^2)(X_1 - Z_1^2), \qquad \beta = 4X_1Y_1^2,$$
$$Z_3 = 2Y_1Z_1, \qquad X_3 = \alpha^2 - 2\beta,$$
$$Y_3 = \alpha(\beta - X_3) - 8Y_1^4.$$

Point Addition in Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2, Z_2)$ be points in Jacobian coordinates on the elliptic curve E. The point addition $P + Q = (X_3, Y_3, Z_3)$, can be computed by:

$$\alpha = Z_1^3 Y_2 - Z_2^3 Y_1, \qquad \beta = Z_1^2 X_2 - Z_2^2 X_1$$

$$Z_3 = Z_1 Z_2 \beta, \qquad X_3 = \alpha^2 - \beta^3 - 2Z_2^2 X_1 \beta^2$$

$$Y_3 = \alpha(Z_2^2 X_1 \beta^2 - X_3) - Z_2^3 Y_1 \beta^3.$$

the cost of the general addition is $12M + 4S$.

Mixed Addition in Jacobian-affine Coordinates

Let $P = (X_1, Y_1, Z_1)$ and $Q = (X_2, Y_2)$ be two points on the elliptic curve E, in Jacobian and affine coordinates, respectively, (or alternatively, with $Q = (X_2, Y_2, 1)$ in Jacobian coordinates). The mixed addition $P + Q = (X_3, Y_3, Z_3)$ is traditionally obtaining as follows, the cost of a mixed addition is $8M + 3S$:

$$\begin{aligned} \alpha &= Z_1^3 Y_2 - Y_1, & \beta &= Z_1^2 X_2 - X_1, \\ Z_3 &= Z_1 \beta, & X_3 &= \alpha^2 - \beta^3 - 2X_1\beta^2, \\ Y_3 &= \alpha(X_1\beta^2 - X_3) - Y_1\beta^3. \end{aligned}$$

Point Tripling in Jacobian Coordinates

Dimitrov et al. introduced a fast tripling formula that cost $10M + 6S$. Let $P = (X_1, Y_1, Z_1)$ be a point in Jacobian coordinates on the elliptic curve E. The triple of the point P, $3P = (X_3, Y_3, Z_3)$, can be computed with $9M + 7S$ as follows:

$$
\begin{aligned}
\alpha &= \theta\omega, & \beta &= 8Y_1^4, \\
\theta &= 3X_1^2 + aZ_1^4 & \omega &= 12X_1Y_1^2 - \theta^2 \\
Z_3 &= Z_1\omega, & X_3 &= 8Y_1^2(\beta - \alpha) + X_1\omega^2, \\
Y_3 &= Y_1\left[4(\alpha - \beta) - (2\beta - \alpha) - \omega^3\right].
\end{aligned}
$$

Chudnovsky Jacobian Coordinates $\mathcal{J}^c$

We see that Jacobian coordinates offer a faster doubling and a slower addition than projective coordinates. In order to make an addition faster, we should represent internally a Jacobian point as the quintuple $(X : Y : Z : Z^2 : Z^3)$. This is called the Chudnovsky Jacobian coordinates and denote by J^c.

Point Addition in Chudnovsky Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1, Z_1^2, Z_1^3)$ and $Q = (X_2, Y_2, Z_2, Z_2^2, Z_2^3)$ be points in Chudnovsky Jacobian coordinates on the elliptic curve E. The point addition $P + Q = (X_3, Y_3, Z_3, Z_3^2, Z_3^3)$ can be computed by the following formula with complexity $11M + 3S$:

$$
\begin{aligned}
U_1 &= X_1 Z_2^2, & U_2 &= X_2 Z_1^2, \\
S_1 &= Y_1 Z_2^3, & S_2 &= Y_2 Z_1^3, \\
H &= U_2 - U_1, & r &= S_2 - S_1, \\
X_3 &= -H^3 - 2U_1 H^2 + r^2, & Y_3 &= -S_1 H^3 + r(U_1 H^2 - X_3), \\
Z_3 &= Z_1 Z_2 H, & Z_3^2 &= Z_3^2, \\
Z_3^3 &= Z_3^3. & &
\end{aligned}
$$

Point Doubling in Chudnovsky Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1, Z_1^2, Z_1^3)$ be a point in Chudnovsky Jacobian coordinates on can be computed $2P = (X_3, Y_3, Z_3)$ by the following formula with complexity $5M + 6S$:

$$\begin{aligned} S &= 4X_1 Y_1^2, & M &= 3X_1^2 + a(Z_1^2)^2, \\ X_3 &= -2S + M^2, & Y_3 &= -8Y_1^4 + M(S - X_3), \\ Z_3 &= 2Y_1 Z_1, & Z_3^2 &= Z_3^2, \\ Z_3^3 &= Z_3^3. \end{aligned}$$

Modified Jacobian Coordinates $\mathcal{J}^{\Updownarrow}$

In order to obtain the faster possible doubling. Cohen "citar" The addition formulas in the modified Jacobian coordinates are the following. Let $P = (X_1, Y_1, Z_1, aZ_1^4)$, $Q = (X_2, Y_2, Z_2, aZ_2^4)$ and $P + Q = (X_3, Y_3, Z_3, aZ_3^4)$

Point Addition in modified Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1, aZ_1^4)$ and $Q = (X_2, Y_2, Z_2, aZ_2^3)$ be points in modified Jacobian coordinates on the elliptic curve E. The point addition $P + Q = (X_3, Y_3, Z_3, aZ_3^2)$ can be computed by the following formula with complexity $?M+?S$:

$$
\begin{aligned}
U_1 &= X_1 Z_2^2, & U_2 &= X_2 Z_1^2,\\
S_1 &= Y_1 Z_2^3, & S_2 &= Y_2 Z_1^3,\\
H &= U_2 - U_1, & r &= S_2 - S_1,\\
X_3 &= -H^3 - 2U_1H^2 + r^2, & Y_3 &= -S_1H^3 + r(U_1H^2 - X_3),\\
Z_3 &= Z_1 Z_2 H, & aZ_3^4 &= aZ_3^4.
\end{aligned}
$$

Point Doubling in modified Jacobian Coordinates

Let $P = (X_1, Y_1, Z_1, aZ_1^4)$ be a point in modified Jacobian coordinates on can be computed $2P = (X_3, Y_3, Z_3, aZ_3^4)$ by the following formula with complexity $M + S$:

$$\begin{aligned} S &= 4X_1Y_1^2, & M &= 3X_1^2 + a(Z_1^4), \\ X_3 &= -2S + M^2, & Y_3 &= -8Y_1^4 + M(S - X_3), \\ Z_3 &= 2Y_1Z_1, & aZ_3^4 &= 2U(aZ_1^4). \end{aligned}$$

Reference

J. López and R. Dahab, *High-speed software multiplication in $\mathbb{F}_{2^m}$*, in: Progress in Cryptology – INDOCRYPT 2000, Lecture Notes in Computer Science, (2000), 203–212.

T. Woolinger and V. Kovtun. *Fast explicit formulae for genus 2 hyperelliptic curves using projective coordinates.* In: International Conference on Information Technology (ITNG'07) IEEE. 2007.

X. Fan, T. Wollinger, and Y. Wang. *Inversion-Free Arithmetic on Genus 3 Hyperelliptic Curves and Its Implementations.* Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC05) 0-7695-2315-3/05 IEEE. 2005.

R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Champan & Hall/CRC Press, 2005.

P. Longa and A. Miri. *Fast and Flexible Elliptic Curves Point Arithmetic over Prime Fields.* IEEE Trans. on Computers. Vol 57, No. 3, March 2008

P. K. Mishra and V. Dimitrov *Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication Using Multibase Number Representation.* ISC 2007, LNCS 4779, pp 390-406, 2007.